

PHASE RETRIEVAL FROM GABOR MEASUREMENTS

IRENA BOJAROVSKA¹ AND AXEL FLINTH¹

ABSTRACT. Compressed sensing investigates the recovery of sparse signals from linear measurements. But often, in a wide range of applications, one is given only the absolute values (squared) of the linear measurements. Recovering such signals (not necessarily sparse) is known as the phase retrieval problem. We consider this problem in the case when the measurements are time-frequency shifts of a suitably chosen generator, i.e. coming from a Gabor frame. We prove an easily checkable injectivity condition for recovery of any signal from all N^2 time-frequency shifts, and for recovery of sparse signals, when only some of those measurements are given.

KEYWORDS. Phase retrieval, PhaseLift, Gabor frames, time-frequency analysis, sparse signals, difference sets

MATHEMATICS SUBJECT CLASSIFICATION. 42C15 · 42A38 · 94A12 · 65T50

1. INTRODUCTION

Phase retrieval, a common problem in a variety of applications including X-Ray crystallography, optical imaging and electron microscopy, is the task of recovering a signal from the squares of the absolute values of its linear measurements. The best one can hope for in this case is to recover the signal up to a unimodular constant, because x and cx , where $|c| = 1$ will always give the same measurements. To fix notation, let $F = (f_i)_{i=1}^m \subseteq \mathbb{K}^N$ be a set of measurement vectors, where \mathbb{K} is \mathbb{R} or \mathbb{C} . Further, let $\mathbb{T} = \{c \in \mathbb{K} : |c| = 1\}$. The measurement process is then given by the map

$$\mathcal{M}_F : \mathbb{K}^N / \mathbb{T} \rightarrow \mathbb{R}_+^m, \quad \mathcal{M}_F(x) = [|\langle x, f_1 \rangle|^2 \quad |\langle x, f_2 \rangle|^2 \quad \dots \quad |\langle x, f_m \rangle|^2]^T.$$

The task is to recover x up to a global phase, given $\mathcal{M}_F(x)$. We say that F *allows phase retrieval*, if the map \mathcal{M}_F is injective.

There are three main directions of questions that one is interested in when looking into this problem:

- **Injectivity:** Which properties of the measurement vectors can give us necessary and/or sufficient conditions on the injectivity of the map \mathcal{M}_F ?
- **Minimal number of measurements:** How many measurements are needed for a set F to allow phase retrieval?
- **Algorithms:** How can one practically find x , given the intensity measurements $\mathcal{M}_F(x)$?

Comprehensive answers to these questions and open problems can be found in [4, 6, 1, 5]. Motivated by different applications, these general questions can also be asked for only a particular type of measurements, and/or signals. In this paper we focus on Gabor, or differently said, short-time Fourier measurements, which are time-frequency shifts of a suitably chosen generator. This type of measurements is of particular interest for many applications in speech and audio processing [21], ptychographical CDI [16] etc. On the signal side, we are looking at the sparsity constraint – a natural assumption that the signal we want to recover has only few non-zero entries, or is a linear combination of few vectors (has sparse representation). The sparsity constraint is a novel paradigm for signal- and image processing, and utilized, in particular, for compressed sensing methodologies [11]. Sparse phase retrieval is studied in [22, 26].

A combination of phase retrieval from Gabor measurements for sparse signals was firstly considered in [10]. The theoretical results there are about the recovery of non-vanishing signals from a full set of N^2 Gabor

¹INSTITUT FÜR MATHEMATIK, TECHNISCHE UNIVERSITÄT BERLIN, GERMANY

E-mail address: bojarovska@math.tu-berlin.de, flinth@math.tu-berlin.de.

The final publication is available at Springer via <http://dx.doi.org/10.1007/s00041-015-9431-0>.

measurements, and some intuition about the difficulty of recovery of sparse signals is given. Numerical results show that recovering sparse signals can be effectively conducted with modification of the GESPAR algorithm [24], using less than N^2 measurements.

In the very recent work [17], both theoretical and numerical investigations show, that $O(N \log^3(N))$ measurements are enough for recovering general signals from block circulant Fourier based measurements, and if the signal is k -sparse, only $O(k \log^5(N))$ measurements. The structure of the measurements is similar to the one of Gabor systems, but at this moment it is not clear how their results transfer to the Gabor setting that we consider here.

In this paper, we investigate the problem of phase retrieval from Gabor measurements, for both full and sparse signals. Our main concern is the question of injectivity. Using the characterization of phase retrievability via the properties of the kernel of the PhaseLift operator [5], we provide a condition on the generator, sufficient for the corresponding Gabor system to allow phase retrieval. We show how this condition can be eased, if the signal that needs to be recovered is non-vanishing. We further provide two exemplary classes of generators, complex random signals and characteristic functions of difference sets, which satisfy the above mentioned condition. The common Gabor generators, which are short windows or Alltop sequences, on the other hand – as we will show – are not suitable for phase retrieval of general signals (they fail to recover sparse signals), this problem was also considered in [17].

Further, we extend the injectivity condition from [5] to the sparse setting, and provide a similar, but more involved condition on the generator which can guarantee us phase retrievability of sparse signals, additionally with less than N^2 measurements. We generalize this result also to signals which are sparse in a Fourier domain. When N is prime, we construct generators such that the Gabor system can do k -sparse phase retrieval from $O(k^3)$ measurements. As we will see, the result can also be interpreted as an injectivity condition for recovery of structured k^2 -sparse vectors from $O(k^3)$ *linear* measurements.

Both the injectivity theorems naturally provide a simple algorithm for recovery of signals up to a global phase. When all N^2 measurements are given, the recovery of any signal is possible by using solely the fast Fourier transform, making the algorithm extremely fast. If some of the measurements are lost, we can employ ℓ_1 minimization to get the signal back. We provide several numerical experiments to test this idea for various settings. Although the number of measurements for recovery in our work is still of relatively high order, the ideas we use are novel, and might be of interest for the community for better understanding of this problem, and its future development.

The remainder of this paper is organized as follows: Section 2 is dedicated to the phase retrievability question for general signals, from all N^2 Gabor measurements. In Section 3, we focus on the sparse setting, and show that k -sparse phase retrieval is possible with order of k^3 Gabor measurements. A detailed description of the algorithm that we propose, and its empirical evaluation is presented in Section 4.

2. AN INJECTIVITY CONDITION FOR ARBITRARY SIGNALS

2.1. Notation and basic objects. We will be working in the signal space \mathbb{C}^N , as a space of complex valued, N periodic functions with integer argument, $x = x(j)$, $j \in \mathbb{Z}$, which therefore always has to be assumed modulo N . We will use the customary domain $[0, \dots, N-1]$ of j , but we will often write $j \in \mathbb{Z}_N$ for convenience. The scalar product between two signals x and y is defined as

$$\langle x, y \rangle = \sum_{j=0}^{N-1} \bar{x}(j)y(j),$$

and the Hilbert Schmidt scalar product between two $N \times N$ matrices A and B as

$$\langle A, B \rangle_{HS} = \text{tr}(A^* B) = \sum_{i \in \mathbb{Z}_N} \langle A e_i, B e_i \rangle.$$

The N -th root of unity will be denoted by $\omega = e^{\frac{2\pi i}{N}}$. We define the (discrete) Fourier transform \hat{x} and the inverse Fourier transform \check{x} of $x \in \mathbb{C}^N$ as follows:

$$\hat{x}(j) = \sum_{n=0}^{N-1} x(n)\omega^{-nj}, \quad \check{x}(j) = \frac{1}{N} \sum_{n=0}^{N-1} x(n)\omega^{nj}.$$

A family of vectors $(\phi_i)_{i=1}^M$ in \mathbb{C}^N is called a *finite frame* for \mathbb{C}^N [7], if there exist constants $0 < A \leq B < \infty$ such that

$$A\|x\|^2 \leq \sum_{i=1}^M |\langle x, \phi_i \rangle|^2 \leq B\|x\|^2 \quad \text{for all } x \in \mathbb{C}^N.$$

If $A = B$ is possible, then $(\phi_i)_{i=1}^M$ is called an *A-tight frame*.

For $p \in \mathbb{Z}_N$, we define the translation operator $T_p : \mathbb{C}^N \mapsto \mathbb{C}^N$ through

$$(T_p x)(n) = x(n - p)$$

Further, we define for $\ell \in \mathbb{Z}_N$, the modulation operator $M_\ell : \mathbb{C}^N \mapsto \mathbb{C}^N$ through

$$(M_\ell x)(n) = \omega^{\ell n} x(n).$$

A *Gabor frame*¹ is the collection of all translations and modulations of a single vector $g \in \mathbb{C}^N$,

$$(M_\ell T_p g)_{\ell,p=0}^{N-1}.$$

For a pair $\lambda = (p, \ell)$ sometimes we will use the short-hand notation $\Pi_\lambda := M_\ell T_p$, and $g_\lambda := \Pi_\lambda g$. The matrices of those operators are unitary, and the collection of them forms a basis of $\mathbb{C}^{N \times N}$ [23], i.e.

$$\langle \Pi_\lambda, \Pi_\mu \rangle_{HS} = N \delta_{\mu, \lambda}. \quad (2.1)$$

We will need the following well-known commutation relations between translations and modulations.

Lemma 2.1. [15] *Let $\lambda = (p, \ell), \mu = (q, j) \in \mathbb{Z}_N^2$. Then, we have*

$$M_\ell T_p = \omega^{\ell p} T_p M_\ell,$$

$$\Pi_\lambda \Pi_\mu = \omega^{-jp} \omega^{\ell q} \Pi_\mu \Pi_\lambda.$$

2.2. Injectivity for full Gabor measurements. As mentioned before, we want to pose the question under what conditions a signal x from some class $\mathcal{C} \subseteq \mathbb{C}^N$ can be recovered from a set of its *Gabor intensity measurements* $(|\langle x, g_\lambda \rangle|^2)_{\lambda \in \Lambda}$, $\Lambda \subseteq \mathbb{Z}_N^2$. Since these measurements are invariant under multiplication with $c \in \mathbb{T} = \{c \in \mathbb{C}, |c| = 1\}$, the best we can hope for is to recover x up to a global phase. If we denote by $\mathbb{C}^N / \mathbb{T}$ the set of equivalence classes under the equivalence relation $x \sim y \Leftrightarrow \exists c \in \mathbb{T} : x = cy$, we can formally pose the problem as follows: Under what conditions on g is the map

$$\mathcal{M}_G : \mathcal{C} / \mathbb{T} \rightarrow \mathbb{R}_+^{|\Lambda|}, \quad x \mapsto (|\langle x, g_\lambda \rangle|^2)_{\lambda \in \Lambda}$$

injective?

Definition 2.1. We say that the Gabor system $G = (g_\lambda)_{\lambda \in \Lambda}$ associated to a generator $g \in \mathbb{C}^N$ is *allowing phase retrieval for \mathcal{C}* (or has the *phase retrieval property*), if the map \mathcal{M}_G is injective.

We start by considering the problem of recovering arbitrary signals from all measurements, i.e. $\mathcal{C} = \mathbb{C}^N$ and $\Lambda = \mathbb{Z}_N^2$. In order to investigate which Gabor frames are allowing phase retrieval for this class, we will use a well known characterization of the phase retrieval property in the complex case, given via the properties of the kernel of the *PhaseLift* operator, also called *super analysis operator* in [5]. For a set of measurement vectors $(f_i)_{i=1}^m$ in \mathbb{C}^N this operator is defined as

$$\mathcal{A} : \mathbb{C}^{N \times N} \rightarrow \mathbb{C}^m, \quad H \mapsto (\langle H, f_i f_i^* \rangle_{HS})_{i=1}^m, \quad (2.2)$$

Note that when H is in the form xx^* , $\langle H, f_i f_i^* \rangle_{HS} = \langle f_i, H f_i \rangle = |\langle x, f_i \rangle|^2$. Also note that the authors of [5] chose the set of Hermitian matrices as the domain of \mathcal{A} . We define \mathcal{A} in this way in order to avoid some

¹We in fact always obtain a frame in this way if $g \neq 0$. The frame is even $N \|g\|^2$ -tight.[23]

technicalities. However, the space of Hermitian matrices is a very natural domain in the context of phase retrieval, as the next theorem suggests.

Theorem 2.1. [5] *A set of measurement vectors $(f_i)_{i=1}^m$ allows phase retrieval if and only if the kernel of the associated map \mathcal{A} does not contain any Hermitian matrices of rank 1 or 2.*

With this theorem, we can prove that the full set of N^2 Gabor intensity measurements allows phase retrieval, as long as a simple condition is satisfied.

Theorem 2.2. *Let $g \in \mathbb{C}^N$ be a generator for which*

$$\langle g, g_\lambda \rangle \neq 0 \quad (2.3)$$

for every $\lambda \in \mathbb{Z}_N^2$. Then the corresponding Gabor frame $G = (g_\lambda)_{\lambda \in \mathbb{Z}_N^2}$ allows phase retrieval.

Proof. Theorem 2.1 suggests that we should investigate $\langle g_\lambda, H g_\lambda \rangle$ for $H \in \mathbb{H}^{N \times N}$. Equality (2.1) implies that

$$H = \frac{1}{N} \sum_{\mu \in \mathbb{Z}_N^2} \langle \Pi_\mu, H \rangle_{HS} \Pi_\mu.$$

If $\mu = (p, \ell)$, we have

$$\langle \Pi_\mu, H \rangle_{HS} = \sum_{i \in \mathbb{Z}_N} \langle \Pi_\mu e_i, H e_i \rangle = \sum_{i \in \mathbb{Z}_N} \left\langle \omega^{\ell(i+p)} e_{i+p}, H e_i \right\rangle = \sum_{i \in \mathbb{Z}_N} \omega^{-\ell i} \langle e_i, H e_{i-p} \rangle = \widehat{\mathcal{H}}_p(\ell),$$

where $\widehat{\mathcal{H}}_p$ denotes the (discrete) Fourier transform of the vector \mathcal{H}_p , defined by $\mathcal{H}_p(i) = H_{i, i-p}$. Note that \mathcal{H}_p is in some sense the p -th 'band' of the matrix H . It hence holds

$$N \langle H, g_\lambda g_\lambda^* \rangle_{HS} = N \langle g_\lambda, H g_\lambda \rangle = \sum_{p, \ell} \left\langle g_\lambda, \widehat{\mathcal{H}}_p(\ell) \Pi_{(p, \ell)} g_\lambda \right\rangle = \sum_{p, \ell} \widehat{\mathcal{H}}_p(\ell) \langle g_\lambda, \Pi_{(p, \ell)} g_\lambda \rangle.$$

If we write $\lambda = (q, j)$, we know by Lemma 2.1 that $\Pi_{(p, \ell)} g_\lambda = \Pi_{(p, \ell)} \Pi_{(q, j)} g = \omega^{-jp} \omega^{\ell q} \Pi_{(q, j)} \Pi_{(p, \ell)} g$. Using this, and the fact that Π_λ is unitary, we arrive at

$$N \langle g_\lambda, H g_\lambda \rangle = \sum_{p, \ell} \omega^{-jp} \omega^{\ell q} \widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle. \quad (2.4)$$

Now, assume that this vanishes for all $\lambda = (q, j) \in \mathbb{Z}_N^2$. Fixing j , we see that the above expression is just the value of the Fourier transform of the vector $V^q \in \mathbb{C}^N$ with p th entry

$$V^q(p) = \sum_{\ell} \omega^{\ell q} \widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle$$

evaluated at j . Since (2.4) equals zero for all j , the vector V^q vanishes for every q . Further, we observe that $V^q(p)$ is N times the value at q of the inverse Fourier transform of the vector $w^p \in \mathbb{C}^N$, where

$$w^p(\ell) = \widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle. \quad (2.5)$$

This expression must therefore be equal to zero for all p and ℓ . With the assumption on the generator, we conclude that all the vectors $\widehat{\mathcal{H}}_p$ must vanish, and therefore also H . H can hence not have rank 1 or 2, and the proof is finished. \square

Carefully going through the argument of the last proof, we see that it shows that the only matrix in the kernel of \mathcal{A} is the zero matrix. Therefore, the proof actually shows that, under the assumption (2.3), \mathcal{A} is an injective map. We use this idea to prove the following theorem.

Theorem 2.3. *Let $g \in \mathbb{C}^N$ be such that $\langle g, g_\lambda \rangle \neq 0$ for all $\lambda \in \mathbb{Z}_N^2$. Then, the N^2 rank-1 operators $(g_\lambda g_\lambda^*)_{\lambda \in \mathbb{Z}_N^2}$ form a frame for $\mathbb{C}^{N \times N}$ (equipped with the Hilbert-Schmidt norm) and hence a basis. The frame bounds are given by*

$$A = N \cdot \min_{\lambda \in \mathbb{Z}^2} |\langle g, g_\lambda \rangle|^2, \quad B = N \cdot \max_{\lambda \in \mathbb{Z}^2} |\langle g, g_\lambda \rangle|^2.$$

Proof. What we need to prove that for every $H \in \mathbb{C}^{N \times N}$

$$A \|H\|_{HS}^2 \leq \sum_{\lambda \in \mathbb{Z}^2} |\langle H, g_\lambda g_\lambda^* \rangle_{HS}|^2 \leq B \|H\|_{HS}^2.$$

In other words, we need to prove that $A \|H\|_{HS}^2 \leq \|\mathcal{A}(H)\|^2 \leq B \|H\|_{HS}^2$, where \mathcal{A} is the PhaseLift operator (2.2). Using the notation of the proof of Theorem 2.2, the formula (2.4) states that the N -tuple $(V^q)_{q=1}^N \in (\mathbb{C}^N)^N$ is obtained by performing inverse Fourier transforms of the columns of the matrix $(N \langle H, g_\lambda g_\lambda^* \rangle_{HS})_{\lambda \in \mathbb{Z}_N^2} = N \mathcal{A}(H)$. Hence, their norms are related as follows:

$$\|N \mathcal{A}(H)\|^2 = \|(\hat{V}^q)_{q=1}^N\|^2 = N \|(V^q)_{q=1}^N\|^2.$$

Using the same argument, we obtain

$$\|(V^q)_{q=1}^N\|^2 = \|(N \check{w}^p)_{p=1}^N\|^2 = \frac{N^2}{N} \|(w^p)_{p=1}^N\|^2 \quad \text{and} \quad \|(\hat{\mathcal{H}}^p)_{p=1}^N\|^2 = N \|(\mathcal{H}^p)_{p=1}^N\|^2.$$

The N -tuples $(\hat{\mathcal{H}}^p)_{p=1}^N$ and $(w^p)_{p=1}^N$ are related through (2.5). Therefore, if we define $\alpha = \min_{\lambda \in \mathbb{Z}^2} |\langle g, g_\lambda \rangle|$, $\beta = \max_{\lambda \in \mathbb{Z}^2} |\langle g, g_\lambda \rangle|$, we have

$$\begin{aligned} \|(w^p)_{p=1}^N\|^2 &= \sum_{(p,\ell) \in \mathbb{Z}_N^2} |w^p(\ell)|^2 = \sum_{(p,\ell) \in \mathbb{Z}_N^2} \left| \hat{\mathcal{H}}_p(\ell) \langle g, g_{p,\ell} \rangle \right|^2 \leq \beta^2 \left\| (\hat{\mathcal{H}}^p)_{p=1}^N \right\|^2 \\ &\geq \alpha^2 \left\| (\hat{\mathcal{H}}^p)_{p=1}^N \right\|^2. \end{aligned}$$

Finally, the matrix H is obtained by merely permuting the elements of the array $(\mathcal{H}^p)_{p=1}^N$. Hence $\|H\|_{HS}^2 = \|(\mathcal{H}^p)_{p=1}^N\|^2$. Combining everything, we obtain

$$\begin{aligned} \|\mathcal{A}(H)\|_{HS}^2 &= \frac{N}{N^2} \|(V^q)_{q=1}^N\|^2 = \|(w^p)_{p=1}^N\|^2 \leq \beta^2 \left\| (\hat{\mathcal{H}}^p)_{p=1}^N \right\|^2 = N \beta^2 \left\| (\mathcal{H}^p)_{p=1}^N \right\|^2 = N \beta^2 \|H\|_{HS}^2 \\ &\geq \alpha^2 \left\| (\hat{\mathcal{H}}^p)_{p=1}^N \right\|^2 = N \alpha^2 \left\| (\mathcal{H}^p)_{p=1}^N \right\|^2 = N \alpha^2 \|H\|_{HS}^2, \end{aligned}$$

which is exactly what we wanted to prove. \square

2.2.1. Non-vanishing vectors. We will now show that if we are interested in recovery of only non-vanishing vectors, weaker conditions on the generator can be assumed.

Definition 2.2. A vector $x \in \mathbb{C}^N$ is called *non-vanishing* (or *full*), if all its entries are nonzero, i.e.

$$x(n) \neq 0, \quad \text{for all } n = 0, \dots, N-1.$$

By \mathcal{C}_f we denote the class of all non-vanishing signals in \mathbb{C}^N .

This situation is much easier to handle, because, intuitively, the non-presence of "holes" in the signals keeps the phases of the entries coupled. We will use the same technique as in Theorem 2.2 to prove that the injectivity condition can be weakened in this setting. Note that we are still assuming that all measurements are known.

Theorem 2.4. Assume that

$$\langle g, g_{p,\ell} \rangle \neq 0 \text{ for } p = 0, 1 \text{ and } \ell \in \mathbb{Z}_N. \quad (2.6)$$

Then the Gabor frame $G = (g_\lambda)_{\lambda \in \mathbb{Z}_N^2}$ allows phase retrieval for \mathcal{C}_f .

Proof. Assume that (2.6) is satisfied, and that x and y are full vectors which are measured equally by the Gabor frame. Then $H := xx^* - yy^*$ is in the kernel of \mathcal{A} , since for every $\lambda \in \mathbb{Z}_N^2$ we have

$$\mathcal{A}(xx^* - yy^*)(\lambda) = \langle g_\lambda, (xx^* - yy^*)g_\lambda \rangle = |\langle g_\lambda, x \rangle|^2 - |\langle g_\lambda, y \rangle|^2 = 0.$$

The proof of Theorem 2.2 then implies that $\hat{\mathcal{H}}_p = 0$ for $p = 0, 1$, i.e. that $\mathcal{H}_0 = \mathcal{H}_1 = 0$. Remembering that $\mathcal{H}_p(i) = H_{i,i-p}$, we arrive at

$$0 = x(i)\bar{x}(i) - y(i)\bar{y}(i) = x(i)\bar{x}(i-1) - y(i)\bar{y}(i-1), \quad i = 0, \dots, N-1.$$

The first equality simply says that $|x(i)| = |y(i)|$, i.e. that there exists numbers $\epsilon_i \in \mathbb{T}$ so that $x(i) = \epsilon_i y(i)$ for all i . Inserting this into the second equation yields

$$0 = y(i)\bar{y}(i-1)(\epsilon_i\bar{\epsilon}_{i-1} - 1).$$

Since all entries of y are assumed to be nonzero, it follows that $\epsilon_i = \epsilon_{i-1}$, i.e. $\epsilon_i = \epsilon_0 =: c \in \mathbb{T}$ for all i . Hence $x = cy$ for a $c \in \mathbb{T}$, and x and y are equal mod \mathbb{T} . \square

Remark 2.1. A similar result was proven in [10]. There, it was only assumed that $\langle g, g_{p,\ell} \rangle \neq 0$ for $p = 0$ and all $\ell \in \mathbb{Z}_N$. However, in this case further constraints on the generators need to be made: g must be a window of length $W \geq 2$, where $N \geq 2W - 1$ and N and $W - 1$ are coprime. Our result, on the other hand, works for more general generators and any N .

2.3. Generators which allow phase retrieval. We will present two types of signals, one random and one deterministic, which satisfy condition (2.3), and thus can be used for phase retrieval of signals from all N^2 Gabor measurements.

2.3.1. Complex random vectors as generators. We start by considering a probabilistic approach, a common strategy in signal recovery in general.

Proposition 2.1. *Let g be a vector in \mathbb{C}^N , randomly distributed according to the complex standard normal distribution. Then, the condition $\langle g, g_\lambda \rangle \neq 0$ for all $\lambda \in \mathbb{Z}_N^2$ is satisfied with probability 1.*

Proof. Since there are only finitely many λ 's, it suffices to prove that $\langle g, \Pi_\lambda g \rangle \neq 0$ with probability 1 for one arbitrary λ . Since Π_λ is a unitary operator, there exists an orthonormal basis $(q_i)_{i=1}^N$ of \mathbb{C}^N and $c_i \in \mathbb{T}$ with

$$\Pi_\lambda = \sum_{i=1}^N c_i q_i q_i^*.$$

If we expand g in this basis, i.e. $g = \sum_i h_i q_i$, then the vector $h \in \mathbb{C}^N$ will also be distributed according to the complex standard normal distribution [13]. We have $\Pi_\lambda g = \sum_i c_i h_i q_i$, and hence

$$\langle g, \Pi_\lambda g \rangle = \sum_{i=1}^N c_i |h_i|^2.$$

In order for g to not satisfy (2.3), the random variable $\mathfrak{h} = \left(|h_i|^2\right)_{i=1}^N$ on \mathbb{R}_+^N must hence lie in the subspace of \mathbb{R}^N defined by

$$\left\{ v : \sum_{i=1}^n c_i v_i = 0 \right\}.$$

Since this space has dimension $N - 1$, the set has Lebesgue measure zero. If we prove that \mathfrak{h} has a distribution which has a density with respect to the Lebesgue measure on \mathbb{R}_+^N which is almost never zero, we are done. This is however not hard to see, since the variables $|h_i|^2 = |a_i|^2 + |b_i|^2$, $i = 1, \dots, N$ are independently distributed according to the χ_2^2 -distribution, which has density $\rho(x) = \frac{1}{2} \exp(-x/2)$ on \mathbb{R}_+ . \square

2.3.2. Difference sets as generators. The second example are so-called difference sets, a construction coming from combinatorial design theory [9]. The set of all modulations of a characteristic function of difference set was shown to achieve the Welch bound in [27]. We will show that the set of all modulations and translations of a difference set has the property desired for phase retrieval.

Definition 2.3. A subset $\mathcal{K} = \{u_1, \dots, u_K\}$ of \mathbb{Z}_N is called an (N, K, ν) *difference set* if the $K(K - 1)$ differences

$$(u_k - u_l) \mod N, \quad k \neq l$$

take all possible nonzero values $1, 2, \dots, N - 1$, with each value appearing exactly ν times.

Example 2.1. Let $N = 7$. The subset $\mathcal{K} = \{1, 2, 4\}$ is then a $(7, 3, 1)$ difference set. We can check this by considering all possible differences modulo 7,

-	1	2	4
1	-	6	4
2	1	-	5
4	3	2	-

and confirming that indeed every value from 1 to 6 appears exactly one time.

Given a difference set \mathcal{K} with parameters (N, K, ν) we denote by $\chi_{\mathcal{K}} \in \{0, 1\}^N$ its characteristic function:

$$\chi_{\mathcal{K}}(j) = \begin{cases} 1, & \text{if } j \in \mathcal{K} \\ 0, & \text{if } j \notin \mathcal{K}. \end{cases}$$

We now prove that if such characteristic functions are used as generators, the corresponding Gabor frames will satisfy (2.3), and hence allow phase retrieval for arbitrary signals.

Proposition 2.2. *Let N be an integer with a prime factorization $N = p_1^{a_1} \dots p_r^{a_r}$. Let \mathcal{K} be a difference set with parameters (N, K, ν) , such that*

$$\nu, K < \min\{p_1, \dots, p_r\}. \quad (2.7)$$

Then, for $g = \chi_{\mathcal{K}}$,

$$\langle g, g_{\mu} \rangle \neq 0 \text{ for every } \mu \in \mathbb{Z}_N^2. \quad (2.8)$$

Proof. Let $\mu = (q, j)$, with both $q, j \neq 0$. By just using the definition of g_{μ} and \mathcal{K} we obtain

$$\langle g, g_{\mu} \rangle = \sum_{n \in \mathbb{Z}_N} g(n)(M_j T_q g)(n) = \sum_{n \in \mathbb{Z}_N} g(n)g(n-q)\omega^{jn} = \sum_{\substack{n \in \mathcal{K} \\ n-q \in \mathcal{K}}} \omega^{jn}. \quad (2.9)$$

Now, taking into account the nature of a difference set, we can conclude that in the set

$$\{n : n \in \mathcal{K}, n - q \in \mathcal{K}\}$$

there will be always exactly ν elements (because for $q \in \mathbb{Z}_N$ there are exactly ν ways to be written as a difference of elements in \mathcal{K} , and $n - (n - q)$ are such differences).

If $\nu = 1$, we are left with a single ω^{jn_0} and then certainly the sum is different from zero.

If $\nu \neq 1$, we have a sum of ν different N -th roots of unity, and we will show that with the given assumptions on the difference set, (2.8) holds. We use the following result from [18] about the vanishing sums of roots of unity. The main theorem in this article states that for any $N = p_1^{a_1} \dots p_r^{a_r}$, the only possible amounts of N -th roots of unity that can sum up to zero is given by $M_1 p_1 + \dots + M_r p_r$. Here the M_i are any non-negative integers (0 is included). Now it is clear that the condition $\nu < \min\{p_1, \dots, p_r\}$ will ensure that we will never have a vanishing sum.

If now $\mu = (0, j)$ the sum will go over the full set \mathcal{K} , and since $K < \min\{p_1, \dots, p_r\}$, again this sum is non vanishing.

Finally, in the last case $\mu = (q, 0)$, we have a sum of ν ones, and therefore we have proven (2.8) for all cases $\mu \in \mathbb{Z}_N^2$. \square

Example 2.2. We now provide some examples of families of difference sets, which satisfy the condition from Proposition 2.2.

Family 1: Quadratic Difference Sets. Let $q = p^r = 3 \pmod{4}$ be a power of a prime and

$$N = q, K = \frac{q-1}{2}, \nu = \frac{q-3}{4}.$$

Then $u = \{t^2 : t \in \mathbb{Z}_N \setminus \{0\}\}$ is a (N, K, ν) difference set. If $r = 1$, condition (2.7) is satisfied.

Family 2: Quartic Difference Sets. Let $p = 4a^2 + 1$ be a prime with a odd, and

$$N = p, K = \frac{p-1}{4}, \nu = \frac{p-5}{16}.$$

$$H_1 = \begin{bmatrix} 0 & & & 1 & & \\ & \ddots & & & & \\ & & & & \ddots & \\ 1 & & & & & \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix} \quad H_2 = \begin{bmatrix} 1 & & & & & \\ & -1 & & & & \\ & & 0 & & & \\ & & & \ddots & & \\ & & & & & 0 \end{bmatrix}$$

FIGURE 1. The matrices H_1 and H_2 used in the proof of Proposition 2.3

Then $u = \{t^4 : t \in \mathbb{Z}_N \setminus \{0\}\}$ is a (N, K, ν) difference set and additionally $K, \nu < N$.

Many other examples can be found in the paper [27], or in the La Jolla Difference Set Repository at <http://www.ccrwest.org/ds.html>.

2.4. Generators which do not allow phase retrieval. We now consider two cases for which condition (2.3) is *not* satisfied, and show that this in fact implies that the Gabor frames do not allow phase retrieval in these cases.

Proposition 2.3. *Let $g \in \mathbb{C}^N$ be a generator such that one of the following two conditions is satisfied*

$$\langle g, g_{\hat{p}, \ell} \rangle = 0, \quad \text{for fixed } \hat{p} \in \mathbb{Z}_N \setminus \{0\} \text{ and all } \ell \in \mathbb{Z}_N. \quad (2.10)$$

$$\langle g, g_{\hat{p}, \ell} \rangle = 0, \quad \text{for } \hat{p} = 0 \text{ and all } \ell \in \mathbb{Z}_N \setminus \{0\}. \quad (2.11)$$

Then, the corresponding Gabor frame $G = (g_\lambda)_{\lambda \in \mathbb{Z}_N^2}$ does not allow phase retrieval for \mathbb{C}_N .

Proof. Let us first assume that condition (2.10) is satisfied. We consider the matrix $H_1 \in \mathbb{H}^{N \times N}$, defined by

$$H_1 = e_0 e_{-\hat{p}}^* + e_{-\hat{p}} e_0^*$$

(e_0 is the 'first unit vector' - remember that we are always considering indices from \mathbb{Z}_N). This matrix has rank 2, and it lies in the kernel of the PhaseLift operator associated to the Gabor frame defined in (2.2). To see this, note that using the notation of the proof of Theorem 2.2 we have

$$\mathcal{H}_p(i) = H_{i, i-p} = \begin{cases} 1 & \text{if } i = 0, p = \hat{p}, \\ 1 & \text{if } i = -\hat{p}, p = -\hat{p}, \\ 0 & \text{else.} \end{cases}$$

In other words, $\mathcal{H}_p = 0$ for all $p \neq \pm \hat{p}$. Since $\langle g, g_{p, \ell} \rangle = \omega^{-\ell p} \overline{\langle g, g_{-p, -\ell} \rangle}$, equation (2.10) also implies $\langle g, g_{-\hat{p}, \ell} \rangle = 0$ for all $\ell \in \mathbb{Z}_N$. These two facts prove that

$$\widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle = 0$$

for all ℓ and p . Using the technique of the proof of Theorem 2.2 backwards, it follows $\mathcal{A}(H_1) = 0$. The matrix H_1 that we have found has rank 2 and it is in the kernel of \mathcal{A} . Therefore, by Theorem 2.1, the Gabor frame can not allow phase retrieval.

Now we assume that (2.11) is satisfied. In this case we define a rank 2 matrix in $\mathbb{H}^{N \times N}$ by

$$H_2 = e_0 e_0^* - e_1 e_1^*.$$

For this matrix, $\mathcal{H}_p = 0$ for $p \neq 0$. Also $\widehat{\mathcal{H}}_0(0) = \sum_i H_{i, i} = 0$. Because of these two facts and the assumption on g , we again have

$$\widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle = 0 \quad \text{for all } (p, \ell) \in \mathbb{Z}_N^2,$$

and H_2 will by the same argument as before be in the kernel of \mathcal{A} . Phase retrieval is again not possible. \square

Example 2.3. We now give two examples, for which the conditions of the previous proposition are satisfied.

Short windows: The condition (2.10) is satisfied if the generator g is a “short window”. More precisely, if $\text{supp } g \subseteq [K_1, K_2]$ for $|K_1 - K_2| < \frac{N}{2}$, then g and $M_\ell T_p g$ will have disjoint supports for some p ’s and hence have a vanishing scalar product. Using a window as a generator is a core idea in short-time Fourier analysis [23].

Alltop sequence: It can be easily shown that the much celebrated Alltop sequence [2], defined as $(\frac{1}{\sqrt{N}}\omega^{n^3})_{n=0}^{N-1}$, has the property (2.11). This generator is often and successfully used in sparse signal recovery from linear Gabor measurements [3, 23].

However, both these families of signals can not be used for phase retrieval, when we are interested in recovery of all signals in \mathbb{C}^N .

3. AN INJECTIVITY CONDITION FOR SPARSE SIGNALS

3.1. Sparse phase retrieval via the PhaseLift operator. We will now consider signals which are sparse in a dictionary. A dictionary D is a set of d vectors in \mathbb{C}^N , and it is identified with the matrix formed when writing the d vectors as its columns. The class of signals which are k -sparse in the dictionary D , or simply kD -sparse signals, is

$$\mathcal{C}_{k,D} = \{x \in \mathbb{C}^N \mid \exists z \in \mathbb{C}^d, \|z\|_0 \leq k, \text{ s.t. } x = Dz\},$$

where $\|z\|_0$ denotes the number of non-zero coefficients in z . If $D = I$, we will omit the dictionary and simply speak of k -sparse vectors \mathcal{C}_k . We will also, to increase readability, speak of kD -phase retrieval instead of phase retrieval for $\mathcal{C}_{k,D}$.

Since sparse vectors in some sense are k - and not N -dimensional, one would hope that the number of measurements required to recover them is smaller (for us, Λ should contain less elements.) This, and other, questions were considered and answered for general measurement vectors in [22] and [26]. A counterpart of Theorem 2.1 in the sparse setting has up to now not been stated and proved. We will prove now an injectivity condition for sparse signals, and then use it for the case of Gabor measurements as in the previous section.

For a given dictionary $D = (d_i)_{i=1}^d$ and a set of indices $\mathcal{K} \subseteq \{1, \dots, d\}$, we denote $W_{\mathcal{K}} = \text{span}\{d_i\}_{i \in \mathcal{K}}$. With the help of this notion, we can characterize sets or measurement vectors which allow kD -phase retrieval. Let \mathcal{A} be the PhaseLift operator defined in (2.2).

Theorem 3.1. *Given the notations from above, the following two statements hold.*

- (1) *If for every \mathcal{K} with $|\mathcal{K}| = 2k$, the kernel of \mathcal{A} does not contain rank 1 or 2 Hermitian matrices whose range is in $W_{\mathcal{K}}$, then the vectors $(f_i)_{i=1}^m$ allow kD -phase retrieval.*
- (2) *If $(f_i)_{i=1}^m$ is allowing kD -phase retrieval, then for every \mathcal{K} with $|\mathcal{K}| = k$, the kernel of \mathcal{A} does not contain rank 1 or 2 Hermitian matrices with range in $W_{\mathcal{K}}$.*

Proof. Let us start by proving (1) by contraposition. Assume that $(f_i)_{i=1}^m$ is not allowing kD -phase retrieval. Then there exists $x \neq y \bmod \mathbb{T}$, both kD -sparse, for which

$$\langle xx^*, f_i f_i^* \rangle_{HS} = |\langle f_i, x \rangle|^2 = |\langle f_i, y \rangle|^2 = \langle yy^*, f_i f_i^* \rangle_{HS},$$

i.e. $xx^* - yy^*$ is a Hermitian matrix in the kernel of \mathcal{A} . If the sparse representations of x and y are given by $x = Dz_x$ and $y = Dz_y$, we see that $\text{ran}(xx^* - yy^*) \subseteq (W_{\text{supp } z_x \cup \text{supp } z_y})$ and further it has rank less than or equal to 2. If we knew that the rank is at least one, $|\text{supp } z_x \cup \text{supp } z_y| \leq 2k$ would imply the claim.

To see that the condition $x \neq y \bmod \mathbb{T}$ in fact implies this, assume, towards a contradiction, that this is not the case, i.e. that $xx^* - yy^* = 0$. Since $x \neq y \bmod \mathbb{T}$, both vectors are non-zero. Hence there exists a vector $v \in \mathbb{C}^N$ such that $\langle x, v \rangle \neq 0$. Multiplying $0 = xx^* - yy^*$ with this v and rearranging terms, we arrive at

$$x = \frac{\langle y, v \rangle}{\langle x, v \rangle} y,$$

i.e. $x = \lambda y$ for a $\lambda \in \mathbb{C}$. Again plugging this into $0 = xx^* - yy^*$ yields $|\lambda| = 1$. This is a contradiction.

Let us now turn to (2). Suppose that there exists a \mathcal{K} such that the kernel \mathcal{A} contains a Hermitian matrix H with rank 1 or 2 with range in $W_{\mathcal{K}}$. By the spectral theorem, there exists an orthonormal basis (φ_j) of \mathbb{C}^N consisting of eigenvectors of H , corresponding to real eigenvalues (λ_j) . It is clear that H may be written as $\sum_j \lambda_j \varphi_j \varphi_j^*$.

Because of the bounded rank and the fact that $H \neq 0$, either one or two of the eigenvalues are non-zero. It is clear that the eigenvectors corresponding to those eigenvalues are vectors in $W_{\mathcal{K}}$, since they form a basis of the range of H . Thus, they are kD -sparse.

Let us first consider the case where only one eigenvalue is different from zero. If we write $x = \sqrt{|\lambda_1|} \varphi_1$, then we have $H = \pm x x^*$ and hence

$$0 = \langle x x^*, f_i f_i^* \rangle = |\langle f_i, x \rangle|^2 = 0.$$

This means that the two kD -sparse vectors x and 0 have the same phaseless measurements, although $x \neq 0 \pmod{\mathbb{T}}$.

The other case is dealt with similarly: here we write $x = \sqrt{|\lambda_1|} \varphi_1$, $y = \sqrt{|\lambda_2|} \varphi_2$ and conclude that $H = \pm x x^* \pm y y^*$, where the signs depend on the signs of the eigenvalues. If the signs are equal, we see that $|\langle f_i, x \rangle|^2 + |\langle f_i, y \rangle|^2 = 0$ and we have again found kD -sparse vectors which are measured 0. If the signs are not equal, we see that $|\langle f_i, x \rangle|^2 - |\langle f_i, y \rangle|^2 = 0$, and hence x and y are measured equally. They are kD -sparse and cannot be equal $\pmod{\mathbb{T}}$, since they are orthogonal. \square

3.2. Signals sparse in the standard basis. Let us start by considering vectors which are sparse in the standard sense, i.e. $D = I$. We will prove a condition under which a subset of our Gabor frame $\{g_\lambda, \lambda \in \mathbb{Z}_N^2\}$ with $\sim k^3$ elements allows k -sparse phase retrieval, when N is prime. For general N , it would still be possible to go below the full set of measurements, N^2 . We will need a special form of the discrete uncertainty principle, which involves the sum of the “spread” of the signal and its Fourier transform. Let us start with a general observation.

Lemma 3.1. *Assume that for all non-zero vectors $f \in \mathbb{C}^N$*

$$\|f\|_0 + \|\hat{f}\|_0 \geq N - \theta_N \quad (3.1)$$

holds for some number θ_N . Then, if f is k -sparse ($\|f\|_0 = k$), and \hat{f} has not less than $\theta_N + k + 1$ zero-entries, then f necessarily has to vanish.

This statement follows immediately by contradiction. The question is whether (3.1) is a reasonable assumption. In [25] it is proved that when N is prime, (3.1) holds with θ_N equal to -1 . For general N , by the standard multiplicative uncertainty principle and the geometric mean-arithmetic mean inequality, one can derive (3.1) with $\theta_N = N - 2\sqrt{N}$. A more involved inequality for general N was obtained in [19] and will be discussed later on.

Before we proceed with a condition on the generator g for sparse phase retrieval, we will first prove a more general statement about recovery of sparse matrices from *linear* measurements, which is interesting on its own. We will be interested in the following class of signals,

$$\mathfrak{H}_K = \{H \in \mathbb{C}^{N \times N} : \exists \mathcal{K} \subseteq [1, \dots, N], |\mathcal{K}| = K : H_{ij} = 0 \text{ if } (i, j) \notin \mathcal{K} \times \mathcal{K}\}.$$

Theorem 3.2. *Let N be such that the uncertainty principle (3.1) holds, and let $\lambda = (p, l) \in \mathbb{Z}_N^2$. Let g have the following property: for each ℓ , the sequence $c_p = (\langle g, g_p, \cdot \rangle)$ formed by letting ℓ run obeys*

$$\theta_N + K + 1 \leq \|c_p\|_0 \leq \hat{k} \quad (3.2)$$

for some K and \hat{k} . Then, for any subsets $A \subseteq \mathbb{Z}_N$, $B \subseteq \mathbb{Z}_N$ with

$$|A| \geq \theta_N + \hat{k} + 1, \quad |B| \geq \theta_N + K^2 - K + 2,$$

the following holds. If a matrix $H \in \mathfrak{H}_K$ satisfies $(\langle g_\lambda g_\lambda^, H \rangle_{HS})_{\lambda \in A \times B} = 0$, then $H = 0$.*

Proof. Let $H \in \mathfrak{H}_K$ satisfy $\langle g_\lambda g_\lambda^*, H \rangle_{HS} = 0$ for $\lambda \in A \times B$ and let \mathcal{K} be such that $H_{ij} = 0$ if $(i, j) \notin \mathcal{K} \times \mathcal{K}$. We will prove that H then must be 0. Recall the notation from the proof in Theorem 2.1, $\mathcal{H}_p(i) = H_{i, i-p}$. Since $H_{i, i-p}$ is zero, if $(i, i-p)$ is not in $\mathcal{K} \times \mathcal{K}$, we can conclude that

$$\mathcal{H}_p(i) = H_{i, i-p} = 0 \quad \text{if } i \notin \mathcal{K} \cap (\mathcal{K} + p).$$

This proves the following properties:

- (1) The vectors \mathcal{H}_p are K -sparse.
- (2) \mathcal{H}_p is zero for all but at most $K^2 - K + 1$ different values for p . To see this, notice first that $\mathcal{H}_p = 0$ if $p \notin \mathcal{K} - \mathcal{K}$. This is because if $\mathcal{H}_p(i) \neq 0$, then $i \in \mathcal{K}$ and there additionally exists a $j \in \mathcal{K}$ with $i = j + p$. It follows $p = i - j \in \mathcal{K} - \mathcal{K}$. And we know that the set $\mathcal{K} - \mathcal{K}$ has at most $|\mathcal{K}|(|\mathcal{K}| - 1) + 1 = K^2 - K + 1$ elements.

Now using the same argument as in the proof of Theorem 2.2, we arrive at

$$0 = N \langle g_\lambda g_\lambda^*, H \rangle = \sum_{p, \ell} \omega^{-jp} \omega^{\ell q} \widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle \quad \text{for all } \lambda = (q, j) \in A \times B. \quad (3.3)$$

Fixing j , the sum in (3.3) is the value at j of the discrete Fourier transform of the vector V^q defined as

$$V^q(p) = \sum_{\ell} \omega^{\ell q} \widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle. \quad (3.4)$$

Because of (2), these vectors are all $(K^2 - K + 1)$ -sparse. Further, (3.3) proves that their Fourier transforms vanish at all $j \in B$, i.e. at $\theta_N + (K^2 - K + 2)$ points. The discrete uncertainty principle (3.1) implies that V^q must equal zero.

Considering (3.4), the fact that $V^q(p) = 0$ proves that the inverse Fourier transform of the vector, which we denote by

$$w^p(\ell) = \widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle$$

vanishes at the values $q \in A$, i.e. at $\theta_N + \hat{k} + 1$ values. Because of our assumption on g , w^p is however \hat{k} -sparse. We can therefore again conclude that

$$\widehat{\mathcal{H}}_p(\ell) \langle g, g_{p, \ell} \rangle = 0 \quad \text{for all } (p, \ell) \in \mathbb{Z}_N^2.$$

Hence, if $\langle g, g_{p, \ell} \rangle \neq 0$, $\widehat{\mathcal{H}}_p(\ell)$ must be 0. Due to our assumption on g , this happens for at least $\theta_N + 2k + 1$ ℓ 's for every p . Because of 1, this is sufficient to prove that $\mathcal{H}_p = 0$ for all p , and H therefore must be 0. \square

We now use the theorem we have just proved, to provide a condition, when a Gabor frame can do k -sparse phase retrieval.

Theorem 3.3. *Let N be such that the uncertainty principle (3.1) holds, and let $\lambda = (p, l) \in \mathbb{Z}_N^2$. Let $g \in \mathbb{C}^N$ be a generator which satisfies the following condition: for each ℓ , the sequence $c_p = (\langle g, g_{p, \cdot} \rangle)$ formed by letting ℓ run obeys*

$$\theta_N + K + 1 \leq \|c_p\|_0 \leq \hat{k} \quad (3.5)$$

for some $K = 2k$ and some \hat{k} . Then, for any subsets $A \subseteq \mathbb{Z}_N$, $B \subseteq \mathbb{Z}_N$ with

$$|A| \geq \theta_N + \hat{k} + 1, \quad |B| \geq \theta_N + (2k)^2 - 2k + 2,$$

the set

$$\{g_\lambda, \lambda \in A \times B\} \quad (3.6)$$

allows k -sparse phase retrieval.

Proof. We will use part (1) of Theorem 3.1 for $D = I$, to show that k -sparse phase retrieval is possible for the system (3.6). Let H be an Hermitian operator with values in $\mathbb{C}_K^N = \{x \in \mathbb{C}^N, \text{supp}(x) \subseteq K\}$ for some K with $|K| = 2k$ for which $\mathcal{A}(H) = 0$ (where \mathcal{A} is the PhaseLift operator associated with (3.6)). We will prove that H must be zero, from which the claim follows. Since the range of H is contained in \mathbb{C}_K^N , we know that $H_{i,j} = 0$ if $i \notin K$. Since $H_{i,j} = \overline{H_{j,i}}$, we also have $H_{i,j} = 0$ if $j \notin K$. We can conclude that $H \in \mathfrak{H}_{2K}$, and by Theorem 3.2 it immediately follows that H is zero, thus the theorem is proved. \square

Remark 3.1. We would like to state the following remarks related to Theorems 3.3 and 3.2.

- (1) If $\theta_N + 4k^2 - 2k + 2 \geq N$, then the same theorem holds for $B = \mathbb{Z}_N$ and any A with $|A| \geq \theta_N + \hat{k} + 1$. We can therefore also in this case reduce the number of measurements from N^2 to $(\theta_N + \hat{k} + 1)N$. Also note that since \hat{k} must not be smaller than $2k$, the theorem does not yield any enhanced results for non-sparse vectors (we need the sequences c_p to be \hat{k} -sparse to reduce the number of measurements, but to have at least $2k$ nonzero elements to ensure injectivity for k -sparse signals).
- (2) We note, that when N is prime, the conditions of Theorem 3.3 become much simpler. Namely,

$$2k \leq \|c_p\|_0 \leq \hat{k},$$

and the sets A and B should fulfill

$$|A| \geq \hat{k}, \quad |B| \geq (2k)^2 - 2k + 1.$$

Thus, for example, if we can find a Gabor system for which the inequality (3.5) is fulfilled as an equality, we will be able to do k -sparse phase retrieval with order of only $O(k \min(N, k^2))$ measurements.

- (3) When N is not prime, we have $\theta_N = N - 2\sqrt{N}$, and the number of needed measurements is not as good as in the prime case, since we obtain

$$|A| \cdot |B| \geq (N - 2\sqrt{N} + \hat{k} + 1)(N - 2\sqrt{N} + (2k)^2 - 2k + 2),$$

but some improvement over N^2 could still be obtained in some cases. Furthermore, an extension of [25] from N prime to general N was published in [19], in the form of the following property:

Let $d_1 < d_2$ be two consecutive divisors of N . If $d_1 \leq k = \|f\|_0 \leq d_2$, then

$$\|\hat{f}\|_0 \geq \frac{N}{d_1 d_2} (d_1 + d_2 - k).$$

Our function θ will in this case explicitly depend on k and be equal to $N - k + \frac{N}{d_1 d_2} (d_1 + d_2 - k)$. The smaller this value is, the less measurements will be needed for k -sparse injectivity.

- (4) Theorem 3.2 is interesting from a different perspective, since \mathfrak{H}_K can be viewed as a set of K^2 -sparse vectors in \mathbb{C}^{N^2} whose sparsity has a special structure. Thus, we have provided a deterministic construction which can theoretically recover those vectors from $O(K^3)$ linear measurements. This is interesting since we know from conventional compressed sensing results [12], that deterministic constructions for stable recovery of K^2 -sparse vectors require $O(K^4)$ linear measurements, whereas random constructions only need $O(K^2)$ measurements. Finding deterministic constructions which can accept sparsity levels on the order higher than the square root of the number of measurements is known as breaking the “square-root bottleneck” [20].

Although in our case, $O(m)$ measurements are needed for sparsity level $m^{2/3}$, one has to bear in mind that the sparsity of the vectors is structured, and that our result is only about the injectivity of the measurements. In particular, we do not prove any recovery guarantees for a specific algorithm. Hence, we have not broken the square-root bottleneck, but the theorem can be seen as a step towards providing new results in this direction.

3.3. Functions window in the Fourier domain as generators. As in the previous section, we now provide an example of a generator g which fulfills our condition.

Proposition 3.1. *Let N be prime and $2k + 1 < N$. Further, let $v \in \mathbb{C}^N$ be a window of length $k + 1$, $v = \chi_{[0,k]}$, where χ_A denotes the characteristic function on the set $A \subseteq \mathbb{Z}_N$. Moreover, let g be defined by $\hat{g} = v$. Then, g satisfies (3.5) with $\hat{k} = 2k + 1$ and therefore, $(2k + 1) \min(4k^2 - 2k + 1, N)$ measurements from the Gabor frame with g as generator will do k -sparse phase retrieval.*

Proof. The Plancherel formula implies that

$$c_p(\ell) = \langle \hat{g}, T_\ell M_p \hat{g} \rangle \quad \text{for all } (p, \ell) \in \mathbb{Z}_N^2$$

Therefore,

$$\langle \hat{g}, T_\ell M_p \hat{g} \rangle = \sum_{m \in \mathbb{Z}_N} \overline{v(m)} v(m - \ell) \omega^{p(m - \ell)} = \sum_{\substack{m \in [0,k] \\ m - \ell \in [0,k]}} \omega^{p(m - \ell)}, \quad (3.7)$$

because of the way we defined v . Note that since $2k < N$, this sum is empty for $|\ell| > k$. Therefore, the sequences c_p are $2k + 1$ -sparse for every p , i.e. \hat{k} -sparse.

It remains to prove that for $|\ell| \leq k$, the expression above is not zero, and hence $\|c_p\|_0 = 2k + 1$. It suffices to consider $\ell \geq 0$, since the other case can be obtained from this one by the substitution $\ell \rightarrow -\ell$. Using the formula for geometric sums, we obtain

$$\sum_{\ell \leq m \leq k} \omega^{p(m - \ell)} = \sum_{n=0}^{k-\ell} \omega^{pn} = \begin{cases} \frac{1 - \omega^{p(k-\ell+1)}}{1 - \omega^p}, & \text{if } p \neq 0, \\ k - \ell + 1, & \text{if } p = 0. \end{cases}$$

The only way this could be zero when $\ell \leq k$ is that $p \neq 0$ and $1 - \omega^{p(k-\ell+1)} = 0$. This would however mean that N is a divisor of $p(k - \ell + 1) \neq 0$. Since N is prime and both p and $(k - \ell + 1)$ are smaller than N , this cannot be the case. Therefore, from Theorem 3.3 we conclude that any subsets $A \subseteq \mathbb{Z}_N$, $B \subseteq \mathbb{Z}_N$ with

$$|A| \geq 2k + 1, \quad |B| \geq (2k)^2 - 2k + 2$$

will do k -sparse phase retrieval. \square

Remark 3.2. The choice of \hat{g} as a characteristic function of $[0, k]$ is not necessary – any generically chosen function with support on $[0, k]$ will also lead to a Gabor system with the same properties. To see this, note that if $|\ell| < k$, the expression (3.7) is a non-trivial polynomial in the variables $\mathbf{re}(v)$, $\mathbf{im}(v)$. Since we have proved that there is a particular choice of v so that all polynomials do not vanish on v , (3.5) will be satisfied for generic v .

Remark 3.3. The matrices provided to prove that the frames considered in Section 2.4 do not allow phase retrieval were all matrices with range in $\mathbb{C}_\mathcal{K}^N$ for a \mathcal{K} with $|\mathcal{K}| = 2$. Hence, the considerations made there in fact proved that the frames are not allowing phase retrieval for \mathcal{C}_k for any $k \geq 2$ (although they might still allow phase retrieval for some other class of signals).

3.4. Signals sparse in Fourier domain. After spending some time discussing the standard sparsity case, it is worth noting that similar results hold for signals which are sparse in the Fourier basis (dictionary) F . Recall the famous commutation relation of F with translations and modulations:

$$\Pi_{(p,\ell)} F = M_\ell T_p F = F T_\ell M_{-p} = \omega^{\ell p} F \Pi_{(-p,\ell)} \quad \text{for all } (p, \ell) \in \mathbb{Z}_N^2. \quad (3.8)$$

This formula allows us to translate the results provided in the previous section to this new setting.

Theorem 3.4. *Let N be such that the uncertainty principle (3.1) holds and F denote the Fourier basis. Let g have the following property: for each ℓ , the sequence $\tilde{c}_\ell = (\langle g, g_{\cdot, \ell} \rangle)$ formed by letting p run obeys*

$$\theta_N + 2k + 1 \leq \|\tilde{c}_\ell\|_0 \leq \hat{k} \quad (3.9)$$

for some k and \hat{k} . Then, for any subsets $A, B \subseteq \mathbb{Z}_N$ with

$$|A| \geq \theta_N + (2k)^2 - (2k) + 2, \quad |B| \geq \theta_N + \hat{k} + 1,$$

the set $\{g_\lambda, \lambda \in A \times B\}$ allows Fk -sparse phase retrieval.

Proof. We would like to apply Theorem 3.1, with $D = F$. Using the notation of that theorem, let H be an arbitrary Hermitian matrix with range contained in $W_{\mathcal{K}}$ for some \mathcal{K} with $|\mathcal{K}| = 2k$. We may write $H = FH^F F^*$ for some other Hermitian H^F , which then has a range which is contained in $\mathbb{C}_{\mathcal{K}}^N$. Let us now proceed as in the proof of Theorem 2.2 and calculate

$$\begin{aligned}\langle \Pi_{(p,\ell)}, H \rangle_{HS} &= \text{tr}(\Pi_{(p,\ell)}^* F H^F F^*) = \text{tr}(F^* \Pi_{(p,\ell)}^* F H^F) = \langle F^* \Pi_{(p,\ell)} F, H^F \rangle_{HS} \\ &= \langle \omega^{\ell p} \Pi_{-p,\ell}, H^F \rangle_{HS} = \omega^{-\ell p} \hat{\mathcal{H}}_{-\ell}^F(p).\end{aligned}$$

We used the commutation relation (3.8), and the fact that F is unitary. We arrive at

$$N \langle g_{\lambda}, H g_{\lambda} \rangle = \sum_{p,\ell} \omega^{-\ell p} \hat{\mathcal{H}}_{-\ell}^F(p) \langle g_{\lambda}, \Pi_{(p,\ell)} g_{\lambda} \rangle.$$

This formula is very similar to (3.3), essentially, the only difference is that the roles of p and ℓ have interchanged. Further, the vectors \mathcal{H}^F have the same properties as the vectors \mathcal{H} in the proof of Theorem 3.4 (since H^F has the same properties as H). These two facts makes it clear that we can use the exact same technique as in that proof to prove this theorem. We leave the details to the reader. \square

It is not hard to construct a concrete example of a generator g which fulfills the condition (3.9). We only have to note that the roles of translations and modulations have been interchanged. Hence, we should no longer use a g which has short support in Fourier domain, but instead one with short support in spatial domain. With this insight, we may use the exact same steps as in the proof of Proposition 3.1 to deduce the following.

Proposition 3.2. *Let N be prime and $2k+1 < N$. Then $(2k+1) \min(4k^2 - 2k + 1, N)$ measurements from a Gabor frame generated by generic windows g of length $k+1$ will do Fk -sparse phase retrieval.*

4. AN ALGORITHM FOR PHASE RETRIEVAL USING GABOR MEASUREMENTS

The idea of the proof of Theorem 3.3 can be used to design an algorithm to reconstruct signals from their Gabor intensity measurements. We start by recovering H , as in the proof, and then we compute the closest rank 1 operator xx^* by spectral decomposition of H . A detailed description is given in Algorithm 1.

Algorithm 1: Simple Gabor Phase Retrieval (SGPR)

Data: A generator $g \in \mathbb{C}^N$, sets $A, B \subseteq \mathbb{Z}_N$, the measurements $b(q, j) = N |\langle x, g_{q,j} \rangle|^2$, $(q, j) \in A \times B$.

Result: An estimate $x_0 \in \mathbb{C}^N$ of x .

- 1 **for** $q = 0 \dots N-1$ **do**
 - └ Solve $\hat{V}^q(j) = b(q, j)$, $j \in B$ for V^q .
- 2 **for** $p = 0 \dots N-1$ **do**
 - └ Solve $N \cdot \hat{w}^p(q) = V^q(p)$, $q \in A$ for w^p .
- 3 **for** $p = 0 \dots N-1$ **do**
 - └ **for** $\ell = 0 \dots N-1$ **do**
 - └ **if** $\langle g, g_{p,\ell} \rangle \neq 0$ **then**
 - └ Set $\hat{\mathcal{H}}_p(\ell) = w^p(\ell) / \langle g, g_{p,\ell} \rangle$.
 - └ Add ℓ to the set Λ_p .
 - └ Solve $\hat{\mathcal{H}}_p(\ell) = w^p(\ell) / \langle g, g_{p,\ell} \rangle$, $\ell \in \Lambda_p$ for \mathcal{H}_p .

Reconstruct H from $H(i, i-p) = \mathcal{H}_p(i)$

Calculate the eigenpair (λ, v) of H corresponding to the largest eigenvalue.

Set $x_0 = \sqrt{\lambda}x$.

In steps (1), (2) and (3) one has to invert a Fourier transform. If all values of the transformed vector are known, one can simply use the standard fast inverse Fourier transform to compute this, and the signal will be

perfectly recovered. If one on the other hand does not know all the values (not all Gabor measurements are given), some other method has to be used, where sparsity can be employed. We have chosen Basis Pursuit [8]. This is a standard approach in compressed sensing when looking for a sparse solution x of the equation $Ax = b$. The algorithm consists of solving the following optimization problem:

$$\min \|x\|_1 \text{ s.t. } Ax = b.$$

We solve this problem with CVX, a package for specifying and solving convex programs [14]. All experiments were conducted on a Intel Core i7-3517U Processor running Windows 8.

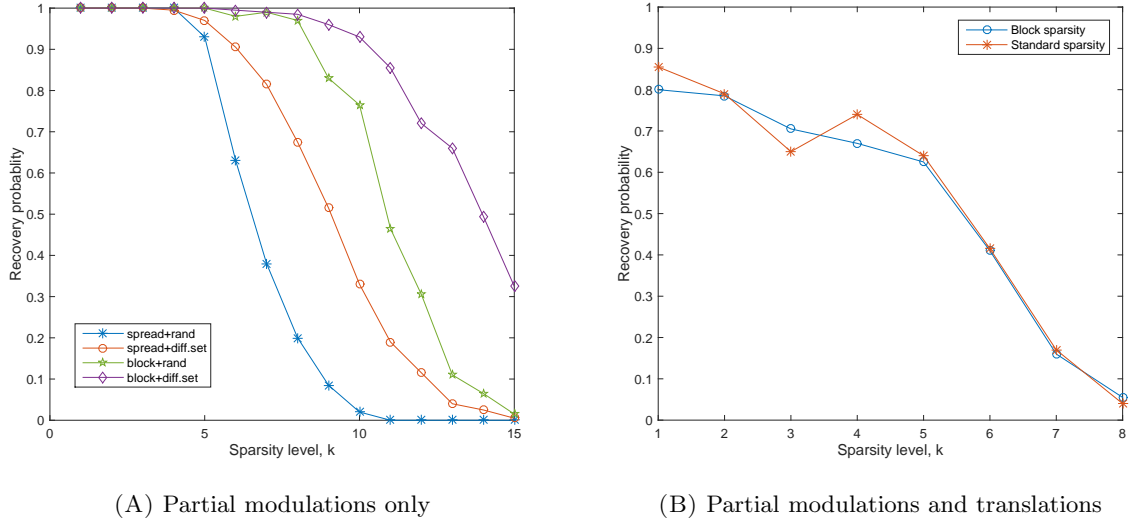


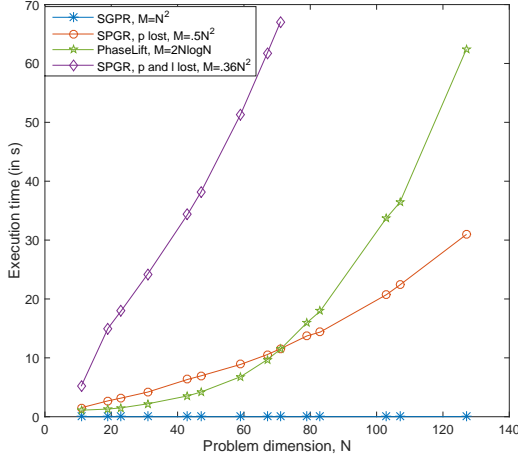
FIGURE 2. Success rate

We now present the results of the numerical experiments for testing Algorithm 1. In Figure 3, we plot the success rate of recovery of sparse signals via Algorithm 1. We have fixed the length of the signal $N = 67$ (a prime which gives $3 \bmod 4$, as needed for difference sets of *Family 1*). We want to recover two types of signals: k -sparse signals, where k non-zero random values are distributed on a random support, and k -sparse block signals, where one random block of k subsequent entries is assigned k random values.

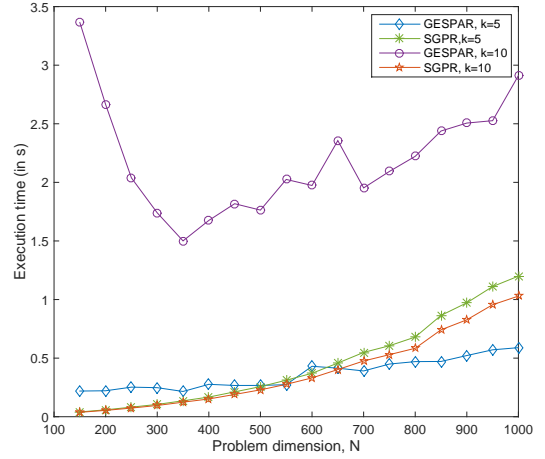
In Figure 2A, we also have chosen two different generators for the Gabor system: a complex random signal, and a characteristic function of a difference set, described in Section 2. Here, we use $0.5N^2$ measurements, namely all N translations, and random $0.5N$ from the modulations. With this setup, we use ℓ_1 minimization only in the Step (1), and in (2) and (3) we use the fast Fourier transform. For a fixed sparsity from 1 to 15, we repeat the experiment $T = 200$ times, and count a trial as successful, if the normalized squared error is smaller than 10^{-2} .

In Figure 2B, we do the same experiment, but we take partial measurements in both directions: translation and modulation. Namely, for $N = 67$, we take $0.52N$ translations, and $0.7N$ modulations at random. The generator here, as described in Proposition 3.1, is a short Fourier window, with length 8. Now, we need to use Basis Pursuit in all steps (1), (2) and (3), which in turn leads to a lower recovery rate. We made $T = 100$ trials for every sparsity level.

In Figure 3A, we test the speed of our algorithm in comparison to the PhaseLift algorithm [6], implemented using the CVX package. We also use Gabor measurements for it, but only $2 \log(N)N$, taken at random. We plot the average execution time over $T = 50$ trials, and see that as the dimension grows, our method becomes faster, although the number of measurements is much larger. Also, if we are using the full set of measurements, the time needed is incomparably smaller to both of the other methods – since then there is



(A) SGPR vs. PhaseLift



(B) SGPR vs. GESPAR

FIGURE 3. Recovery time

no minimization problem included. In this case, also, we will always recover the signal with probability 1, independently of the sparsity level.

In Figure 3B, we compare the execution time of Algorithm 1 from all N^2 measurements to the GESPAR algorithm [24], a greedy algorithm for recovery of sparse signals from Fourier intensity measurements (in our experiment we use $2N$ measurements). This algorithm is very fast for high dimensions, but since it is iterative, it becomes slower as the sparsity increases for a fixed dimension of the signal. We illustrate this behavior in Figure 3B, where for every dimension, we measure the average time of recovery of signals with sparsity $k = 5$ and $k = 10$. We see that the GESPAR algorithm is faster, when we want to recover a signal which has only 5 nonzeros, but if this number is larger, our algorithm becomes faster than the GESPAR, since it does not strongly depend on the sparsity level.

We would like to mention that our algorithm for all N^2 measurements is also stable to additive noise in the measurements. This follows from Theorem 2.3 and can be intuitively explained by the fact that the only troublesome part is the division in Step (3). If the generator g is such, that the values $\langle g, g_{p,l} \rangle$ are bounded away from zero, one can guarantee robustness to noise. For the recovery from less than N^2 measurements, we leave the detailed investigation on this matter for future work.

ACKNOWLEDGMENT

The authors would like to thank Gitta Kutyniok and Peter Jung for fruitful discussions and remarks, and Martin Schäfer, who assisted in the proof-reading of the manuscript. I. B. acknowledges support by the Berlin Mathematical School. A. F. acknowledges support by Deutsche Forschungsgemeinschaft (DFG) Grant KU 1446/18-1 and by the Deutscher Akademischer Austausch Dienst (DAAD).

REFERENCES

- [1] B. Alexeev, A. S. Bandeira, M. Fickus, and D. G. Mixon. Phase retrieval with polarization. *SIAM J. Imag. Sci.*, 7(1):35–66, 2014.
- [2] W. O. Alltop. Complex sequences with low periodic correlations. *IEEE Trans. Inform. Theory*, 26(3):350–354, 1980.
- [3] W. U. Bajwa, R. Calderbank, and S. Jafarpour. Why Gabor frames? Two fundamental measures of coherence and their role in model selection. *J. Commun. Networks*, 12(4):289–307, 2010.
- [4] R. Balan, P. Casazza, and D. Edidin. On signal reconstruction without phase. *Appl. Comput. Harmon. Anal.*, 20(3):345–356, 2006.

- [5] A. S. Bandeira, J. Cahill, D. G. Mixon, and A. A. Nelson. Saving phase: Injectivity and stability for phase retrieval. *Appl. Comput. Harmon. Anal.*, 37(1):106–125, 2014.
- [6] E. J. Candès, Y. C. Eldar, T. Strohmer, and V. Voroninski. Phase retrieval via matrix completion. *SIAM J. Imag. Sci.*, 6(1):199–225, 2013.
- [7] P. G. Casazza and G. Kutyniok, editors. *Finite frames: Theory and applications*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York, 2013.
- [8] S. S. Chen, D. L. Donoho, and M. A. Saunders. Atomic decomposition by basis pursuit. *SIAM J. Sci. Comput.*, 20(1):33–61, 1998.
- [9] J. H. Dinitz and D. R. Stinson. *Contemporary design theory: A collection of Surveys*, volume 26. John Wiley & Sons, 1992.
- [10] Y. Eldar, P. Sidorenko, D. Mixon, S. Barel, and O. Cohen. Sparse phase retrieval from short-time Fourier measurements. *IEEE Signal Process. Lett.*, 22(5), 2015.
- [11] Y. C. Eldar and G. Kutyniok, editors. *Compressed sensing*. Cambridge University Press, Cambridge, 2012. Theory and applications.
- [12] S. Foucart and H. Rauhut. *A mathematical introduction to compressive sensing*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York, 2013.
- [13] R. G. Gallager. Circularly-symmetric gaussian random vectors, 2008.
- [14] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. <http://cvxr.com/cvx>, Mar. 2014.
- [15] K. Gröchenig. *Foundations of time-frequency analysis*. Applied and Numerical Harmonic Analysis. Birkhäuser Boston, Inc., Boston, MA, 2001.
- [16] M. Guizar-Sicairos and J. R. Fienup. Phase retrieval with transverse translation diversity: a nonlinear optimization approach. *Opt. Express*, 16(10):7264–7278, 2008.
- [17] M. Iwen, A. Viswanathan, and Y. Wang. Fast phase retrieval for high-dimensions. *arXiv preprint arXiv:1501.02377*, 2015.
- [18] T. Y. Lam and K. H. Leung. On vanishing sums of roots of unity. *J. Algebra*, 224(1):91–109, 2000.
- [19] R. Meshulam. An uncertainty inequality for finite abelian groups. *European J. Combin.*, 27(1):63–67, 2006.
- [20] D. G. Mixon. Explicit matrices with the restricted isometry property: Breaking the square-root bottleneck. *arXiv preprint arXiv:1403.3427*, 2014.
- [21] S. H. Nawab, T. F. Quatieri, and J. S. Lim. Signal reconstruction from short-time Fourier transform magnitude. *IEEE Trans. Acoust. Speech Signal Process.*, 31(4):986–998, 1983.
- [22] H. Ohlsson and Y. C. Eldar. On conditions for uniqueness in sparse phase retrieval. In *IEEE Int. Conf. Acoust. Speech Signal Process. 2014 (ICASSP)*, pages 1841–1845. IEEE, 2014.
- [23] G. E. Pfander. Gabor frames in finite dimensions. In *Finite frames*, pages 193–239. Springer, 2013.
- [24] Y. Shechtman, A. Beck, and Y. C. Eldar. GESPAR: Efficient phase retrieval of sparse signals. *IEEE Trans. Signal Process.*, 62(4):928–938, 2014.
- [25] T. Tao. An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett.*, 12(1):121–128, 2005.
- [26] Y. Wang and Z. Xu. Phase retrieval for sparse signals. *Appl. Comput. Harmon. Anal.*, 37(3):531–544, 2014.
- [27] P. Xia, S. Zhou, and G. B. Giannakis. Achieving the Welch bound with difference sets. *IEEE Trans. Inf. Theory*, 51(5):1900–1907, 2005.